

了解随机无线加密流程

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[描述](#)

[步骤](#)

[实验室重现的详细信息](#)

[OWE FLOW](#)

[原始信标帧](#)

[隐藏的SSID信标](#)

[从客户端发送到OWE转换SSID的探测请求](#)

[从AP发送到客户端的探测响应](#)

[开放式身份验证](#)

[从客户端到AP的关联请求](#)

[从AP发送到客户端的关联响应](#)

[密钥交换](#)

[L2身份验证成功](#)

[IP学习状态](#)

[客户端处于运行状态](#)

[不支持OWE加密的客户端](#)

[快速过渡信息](#)

[PSK/dot1x不支持OWE](#)

[故障排除](#)

[RA跟踪和EPC \(嵌入式数据包捕获 \)](#)

[AIR PCAP](#)

[漫游](#)

简介

本文档介绍OWE转换流程及其在Catalyst 9800无线LAN控制器(WLC)上的工作方式。

先决条件

要求

Cisco 建议您了解以下主题：

- 如何配置9800 WLC (接入点[AP]) 以实现基本操作
- 如何配置WLAN和策略配置文件。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- C9800-80、Cisco IOS® XE 17.12.4，还在Cisco IOS® XE 17.9.6中进行了测试
- AP型号：C9136I，已检查本地和灵活连接模式。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

描述

- OWE（机会性无线加密）是IEEE 802.11的扩展，为无线介质提供加密。基于OWE的身份验证的目的是避免AP和客户端之间的开放式非安全无线连接。
- OWE使用基于Diffie-Hellman算法的加密来设置无线加密。
- 使用OWE时，客户端和AP在访问过程中执行Diffie-Hellman密钥交换，并将生成的成对密钥与4次握手配合使用。
- 使用OWE可增强部署基于开放式或共享PSK的网络的无线网络安全。

步骤

1. 配置一个不带任何加密/安全的开放式WLAN并启用广播。
2. 使用OWE安全设置配置另一个SSID，并在transition-mode-wlan-id中映射开放式WLAN ID号。禁用此OWE过渡SSID中的广播SSID选项。
3. 在OPEN WLAN“transition-mode-wlan-id”字段中映射OWE转换WLAN ID号。

实验室重现的详细信息

- 开放式SSID名称：未结欠款
- OWE转换SSID名称：OWE-Transition
- BSSID OF OPEN-OWE:40:ce:24:dd:2e:87
- OWE-Transition的BSSID:40:ce:24:dd:2e:8f

OWE FLOW

1. 可以广播开放式SSID的信标。您可以在AIR PCAP中通过其SSID名称看到它。
2. 我们还可以在AIR PCAP中看到名为“Wildcard”（通配符）而不是其自身SSID名称的启用隐藏安全的SSID。
3. 客户端收到开放SSID的信标帧后，如果它有或支持OWE，则它可开始向OWE过渡SSID（即启用安全功能的SSID而不是开放式SSID）发送探测请求。
4. OWE支持的客户端可以从转换SSID获取探测响应。

5. 客户端和AP之间可以进行OPEN身份验证。
6. 客户端可以向AP发送包含DH密钥交换详细信息的关联请求，并将生成的成对密钥用于4次握手。
7. AP可以发送关联响应。
8. AP和客户端设备之间可能会发生四次握手。
9. 密钥管理成功后，L2 PSK可以成功。
10. 客户端可以从DHCP、ARP等获取IP。
11. 客户端可以进入RUN状态。
12. 如果客户端设备不支持OWE，则它可以向OPEN SSID自身发送探测请求，并且可以直接获取IP，而不是进入RUN状态。

原始信标帧

- 此处，AIR PCAP显示SSID“OPEN-OWE”广播（信标帧）。包含过渡SSID详细信息，称为“OWE-Transition”。

No.	Time	Source	Destination	Protocol	Length	Info
47285	2025-01-21 09:53:18.259879	Cisco_dd:2e:87	Broadcast	802.11	376	Beacon frame, SN=1157, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"

```

> Frame 47285: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
- IEEE 802.11 Wireless Management
  - Fixed parameters (12 bytes)
  - Tagged parameters (300 bytes)
    - SSID parameter set: "OPEN-OWE"
      - Tag Number: SSID parameter set (0)
      - Tag length: 8
      - SSID: "OPEN-OWE"
    - Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    - Tag: DS Parameter set: Current Channel: 48
    - Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    - Tag: Country Information: Country Code IN, Environment All
    - Tag: Power Constraint: 0
    - Tag: QBSS Load Element 802.11e CCA Version
    - Tag: RM Enabled Capabilities (5 octets)
    - Tag: HT Capabilities (802.11n D1.10)
    - Tag: HT Information (802.11n D1.10)
    - Tag: Extended Capabilities (8 octets)
    - Tag: VHT Capabilities
    - Tag: VHT Operation
    - Tag: Tx Power Envelope
    - Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    - Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
    - Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled
    - Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
    - Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
    - Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode
      - Tag Number: Vendor Specific (221)
      - Tag length: 25
      - OUI: 50:6f:9a (Wi-Fi Alliance)
      - Vendor Specific OUI Type: 28
      - BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
      - SSID length: 14
      - SSID: OWE-Transition
  
```

图1:开放式SSID的信标帧

隐藏的SSID信标

- 根据WLAN配置，此“OWE-Transition”SSID禁用“广播”，但是，您可以看到包含SSID名称“Wildcard”的AIR PCAP中的隐藏SSID信标。但是，如果检查该数据包，它包含OWE-Transition详细信息。
- 使用此数据包（例如“40:ce:24:dd:2e:8f”）获取隐藏SSID的BSSID，并在数据包捕获中搜索它。
- 在此数据包中，它显示SSID“Missing”，并包含其转换SSID“OPEN-OWE”和BSSID“40:ce:24:dd:2e:87”。

No.	Time	Source	Destination	Protocol	Length	Info
22581	2025-01-21 09:52:23.230007	Cisco_dd:2e:8f	Broadcast	802.11	390	Beacon frame, SN=2483, FN=0, Flags=.....C, BI=100, SSID=wildcard (Broadcast)
> Frame 22581: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Beacon frame, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (12 bytes) > Tagged parameters (314 bytes) > Tag: SSID parameter set: Wildcard SSID Tag Number: SSID parameter set (0) Tag length: 0 SSID: <MISSING> > Tag: Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec] > Tag: DS Parameter set: Current Channel: 48 > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap > Tag: Country Information: Country Code IN, Environment All > Tag: Power Constraint: 0 > Tag: RSN Information > Tag: QoS Load Element 802.11e CCA Version > Tag: RM Enabled Capabilities (5 octets) > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: Tx Power Envelope > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11) > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44) > Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode Tag Number: Vendor Specific (221) Tag length: 19 OUI: 50:6f:9a (Wi-Fi Alliance) Vendor Specific OUI Type: 28 BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) SSID length: 8 SSID: OPEN-OWE						

图2:隐藏SSID - OWE转换

从客户端发送到OWE转换SSID的探测请求

- 根据信标帧“OPEN-OWE” SSID，客户端知道需要连接的其他SSID详细信息，在本场景中为“OWE-Transition”。如果客户端能够支持OWE加密，则它可以将探测请求发送到“OWE-Transition”SSID并获得响应。
- 探测请求发送到OWE-Transition BSSID "40:ce:24:dd:2e:8f"，并收到响应。在此探测响应数据包内，您还可以看到OPEN-OWE SSID详细信息。

No.	Time	Source	Destination	Protocol	Length	Info
8509	2025-01-21 09:51:57.318400	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	197	Probe Request, SN=0, FN=0, Flags=.....C, SSID="OWE-Transition"
8510	2025-01-21 09:51:57.318412		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8511	2025-01-21 09:51:57.319223	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	398	Probe Response, SN=782, FN=0, Flags=.....C, BI=100, SSID="OWE-Transition"
8512	2025-01-21 09:51:57.319233		Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
> Frame 8509: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Probe Request, Flags:C > IEEE 802.11 Wireless Management > Tagged parameters (133 bytes) > Tag: SSID parameter set: "OWE-Transition" Tag Number: SSID parameter set (0) Tag length: 14 SSID: "OWE-Transition" > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec] > Tag: DS Parameter set: Current Channel: 48 > Tag: HT Capabilities (802.11n D1.10) > Tag: Extended Capabilities (11 octets) > Tag: VHT Capabilities > Ext Tag: HE Capabilities > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity Experience Tag Number: Vendor Specific (221) Tag length: 7 OUI: 50:6f:9a (Wi-Fi Alliance) Vendor Specific OUI Type: 22 MBO/OCE attribute: 030102 (Cellular Data Capabilities) > Tag: Vendor Specific: Microsoft Corp.: Unknown 8						

图3:探测请求

从AP发送到客户端的探测响应

- 客户端收到SSID“OWE-Transition”的探测响应，但是它在WiFi Alliance中有其原始SSID详细信息“OPEN-OWE”。

8509	2025-01-21 09:51:57.318400	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	197	Probe Request, SN=0, FN=0, Flags=.....C, SSID="OWE-Transition"
8510	2025-01-21 09:51:57.318412	ee:13:e8:a8:cd:5b	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8511	2025-01-21 09:51:57.319223	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	398	Probe Response, SN=782, FN=0, Flags=.....C, BI=100, SSID="OWE-Transition"
8512	2025-01-21 09:51:57.319233	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C


```

> Frame 8511: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Probe Response Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  > Tagged parameters (322 bytes)
    > Tag: SSID parameter set: "OWE-Transition"
      Tag Number: SSID parameter set (0)
      Tag length: 14
      SSID: "OWE-Transition"
        > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
        > Tag: DS Parameter set: Current Channel: 48
        > Tag: Country Information: Country Code IN, Environment All
        > Tag: Power Constraint: 0
        > Tag: RSN Information
        > Tag: QoS Load Element 802.11e CCA Version
        > Tag: RM Enabled Capabilities (5 octets)
        > Tag: HT Capabilities (802.11n D1.10)
        > Tag: HT Information (802.11n D1.10)
        > Tag: Extended Capabilities (8 octets)
        > Tag: VHT Capabilities
        > Tag: VHT Operation
        > Tag: Tx Power Envelope
        > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
        > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
        > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled
        > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
        > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
        > Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode
          Tag Number: Vendor Specific (221)
          Tag length: 19
          OUI: 50:6f:9a (Wi-Fi Alliance)
          Vendor Specific OUI Type: 28
          BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
          SSID length: 8
          SSID: OPEN-OWE

```

图4:探测响应

开放式身份验证

- 获得探测响应后，客户端和AP之间可能会进行OPEN身份验证，以在关联之前检查客户端的wifi详细信息/功能。

No.	Time	Source	Destination	Protocol	Length	Info
8517	2025-01-21 09:51:57.327250	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	70	Authentication, SN=1, FN=0, Flags=.....C
8518	2025-01-21 09:51:57.327265		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
> Frame 8517: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Authentication, Flags:C Type/Subtype: Authentication (0x000b) > Frame Control Field: 0xb000 .000 0000 0011 1100 = Duration: 60 microseconds > Receiver address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > Destination address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > Transmitter address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b) > Source address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b) > BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) 0000 = Fragment number: 0 0000 0000 0001 = Sequence number: 1 Frame check sequence: 0x928f3869 [unverified] [FCS Status: Unverified] [WLAN Flags:C]						
> IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) Authentication Algorithm: Open System (0) Authentication SEQ: 0x0001 Status code: Successful (0x0000)						

No.	Time	Source	Destination	Protocol	Length	Info
8520	2025-01-21 09:51:57.327278	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	70	Authentication, SN=783, FN=0, Flags=.....C
8521	2025-01-21 09:51:57.327349		Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Transition"
8523	2025-01-21 09:51:57.329466		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
> Frame 8520: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Authentication, Flags:C Type/Subtype: Authentication (0x000b) > Frame Control Field: 0xb000 .000 0000 0011 1100 = Duration: 60 microseconds > Receiver address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b) > Destination address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b) > Transmitter address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > Source address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) 0000 = Fragment number: 0 0011 0000 1111 = Sequence number: 783 Frame check sequence: 0xc3c21908 [unverified] [FCS Status: Unverified] [WLAN Flags:C]						
> IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) Authentication Algorithm: Open System (0) Authentication SEQ: 0x0002 Status code: Successful (0x0000)						

图5:探测成功后执行OPEN身份验证

从客户端到AP的关联请求

- 请注意，在此数据包中，客户端可以附加用于加密的Diffie-Hellman参数值。

No.	Time	Source	Destination	Protocol	Length	Info
8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Transition"
8523	2025-01-21 09:51:57.329466		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
> Frame 8522: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Request, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (4 bytes) > Tagged parameters (269 bytes) Tag: SSID parameter set: "OWE-Transition" Tag Number: SSID parameter set (0) Tag length: 14 SSID: "OWE-Transition" > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: Power Capability Min: -20, Max: 14 > Tag: Supported Channels > Tag: HT Capabilities (802.11n D1.10) > Tag: RSN Information > Tag: RM Enabled Capabilities (5 octets) > Tag: Supported Operating Classes > Tag: Extended Capabilities (11 octets) > Tag: VHT Capabilities > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Microsoft Corp.: WMN/WME: Information Element Ext Tag: OWE Diffie-Hellman Parameter Ext Tag length: 34 (Tag len: 35) Ext Tag Number: OWE Diffie-Hellman Parameter (32) Group: 256-bit random ECP group (19) Public Key: 7c2782ba4c77a98c7076d1fa2e3493347ec16d4c64345dccf8b9bb68b212ff31						

图6:关联请求

- 在RA跟踪中，您可以开始查看关联阶段的客户端日志，

2025/01/21 15:21:57.391071821 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391117645 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b

从AP发送到客户端的关联响应

No.	Time	Source	Destination	Protocol	Length	Info
8527	2025-01-21 09:51:57.333153	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	245	Association Response, SN=784, FN=0, Flags=.....C
8528	2025-01-21 09:51:57.333161	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C

> Frame 8527: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Association Response, Flags:

Type/Subtype: Association Response (0x0001)

> Frame Control Field: 0x1000

.000 0000 0011 1100 = Duration: 60 microseconds

> Receiver address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)

> Destination address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)

> Transmitter address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

> Source address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

> BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

.... 0000 = Fragment number: 0

0011 0001 0000 = Sequence number: 784

Frame check sequence: 0x7fbed111 [unverified]

[FCS Status: Unverified]

[WLAN Flags:

> IEEE 802.11 Wireless Management

> Fixed parameters (6 bytes)

> Capabilities Information: 0x1111

Status code: Successful (0x0000)

..00 0000 0000 0001 = Association ID: 0x0001

> Tagged parameters (175 bytes)

> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

> Tag: RSN Information

> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

> Tag: HT Capabilities (802.11n D1.10)

> Tag: HT Information (802.11n D1.10)

> Tag: Extended Capabilities (8 octets)

> Tag: VHT Capabilities

> Tag: VHT Operation

> Tag: RM Enabled Capabilities (5 octets)

> Tag: BSS Max Idle Period

图7:关联响应

2025/01/21 15:21:57.391334260 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392296819 {wncd_x_R0-0}{1}: [dot11] [21675]: (note): MAC: ee13.e8a8.cd5b Association

密钥交换

AP和客户端设备之间可能会发生4次握手。

Key-1由AP发送

客户端发送的密钥2

Key-3由AP发送

Key-4由客户端发送

No.	Time	Source	Destination	Protocol	Length	Info
8540	2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193	Key (Message 1 of 4)
8541	2025-01-21 09:51:57.360930	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8542	2025-01-21 09:51:57.363375	Cisco_dd:2e:87	Broadcast	802.11	376	Beacon frame, SN=3335, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215	Key (Message 2 of 4)
8544	2025-01-21 09:51:57.365603	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267	Key (Message 3 of 4)
8546	2025-01-21 09:51:57.366929	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8547	2025-01-21 09:51:57.368482	Cisco_dd:2e:86	Broadcast	802.11	376	Beacon frame, SN=3336, FN=0, Flags=.....C, BI=100, SSID="newssid"
8548	2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171	Key (Message 4 of 4)
8549	2025-01-21 09:51:57.373334	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C

> Frame 8540: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)
 > Radiotap Header v0, Length 34
 > 802.11 radio information
 > IEEE 802.11 QoS Data, Flags:F.C
 > Logical-Link Control
 > 802.1X Authentication
 Version: 802.1X-2004 (2)
 Type: Key (3)
 Length: 117
 Key Descriptor Type: EAPOL RSN Key (2)
 [Message number: 1]
 > Key Information: 0x0088
 Key Length: 16
 Replay Counter: 0
 WPA Key Nonce: 1728f47ac2427421f37f1b43b6f69471eaf8a1a78feb2e1083d188c5a2e05ded
 Key IV: 00000000000000000000000000000000
 WPA Key RSC: 00000000000000000000000000000000
 WPA Key ID: 00000000000000000000000000000000
 WPA Key MIC: 00000000000000000000000000000000
 WPA Key Data Length: 22
 > WPA Key Data: dd14000fac0421b550dab0a335c355e7f4daa4a633af

图8:4次握手

```

2025/01/21 15:21:57.392538716 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392557538 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392640494 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b L2
2025/01/21 15:21:57.394830551 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b Cli
2025/01/21 15:21:57.395171903 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b Cli
2025/01/21 15:21:57.420590731 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b Cli

2025/01/21 15:21:57.420706435 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.420775720 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.426548998 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.426727805 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434078994 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (note): MAC: ee13.e8a8.cd5b

```

L2身份验证成功

```

2025/01/21 15:21:57.434111288 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434250308 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b L2
2025/01/21 15:21:57.434286035 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b Cli
2025/01/21 15:21:57.434308953 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b

```

IP学习状态

```
2025/01/21 15:21:57.434789679 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.436611026 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.437508189 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.534166453 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interface
2025/01/21 15:21:57.535325325 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.535874658 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interface
2025/01/21 15:21:57.536500021 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

客户端处于运行状态

```
2025/01/21 15:21:57.537017277 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
```

不支持OWE加密的客户端

- 通过检查信标帧本身，客户端可以了解它们是否能够支持此加密方法。如果不受支持，则它只需发送探测请求到开放式SSID“OPEN-OWE”，并可执行正常的开放身份验证，获取IP地址，然后进入RUN状态。

```
2025/01/16 15:36:06.178370757 {wncd_x_R0-2}{1}: [client-orch-sm] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:06.209288788 {wncd_x_R0-2}{1}: [dot11] [17332]: (note): MAC: d037.4587.8f35 Associati
2025/01/16 15:36:06.248651191 {wncd_x_R0-2}{1}: [client-auth] [17332]: (note): MAC: d037.4587.8f35 Ope
2025/01/16 15:36:06.248751507 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.281808554 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.303307756 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:10.305041414 {wncd_x_R0-2}{1}: [client-iplearn] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:10.305777492 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
```

快速过渡信息

- 我们只能在OPEN身份验证或Webauth(CWA/LWA/EWA)中配置OWE。
- OWE转换不支持FT。
- 如果启用FT，则会收到此错误消息，

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☐ WPA + WPA2

☐ WPA2 + WPA3

☒ WPA3

☐ Static WEP

☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

GTK Randomize

☐

WPA2 Policy

☐

WPA3 Policy

☒

Transition Disable

☐

WPA2/WPA3 Encryption

AES(CCMP128)

☒

GCMP128

☐

CCMP256

☐

GCMP256

☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

Fast Transition needs to be disabled

SAE

☐

OWE

☒

802.1X-SHA256

☐

FT + SAE

☐

FT + 802.1X

☐

Transition Mode WLAN ID

9

Cancel

Update & Apply to Device

图9:在OWE转换SSID中启用FT时出现错误消息

PSK/dot1x不支持OWE

我们无法在这些组合中启用OWE，

1. 802.1x或FT+802.1x
2. PSK或FT+PSK或PSK-SHA256
3. SAE或FT+SAE
4. 802.1x-SHA256或FT+802.1x-SHA256

如果您尝试启用其中任何一种方法，则会收到错误消息，

General **Security** Advanced Add To Policy Tags**Layer2** Layer3 AAA☐ WPA + WPA2☐ WPA2 + WPA3☒ WPA3☐ Static WEP☐ NoneMAC Filtering ☐Lobby Admin Access ☐

WPA Parameters

WPA Policy ☐GTK Randomize ☐WPA2 Policy ☐WPA3 Policy ☒Transition Disable ☐

WPA2/WPA3 Encryption

AES(CCMP128) ☒GCMP128 ☐CCMP256 ☐GCMP256 ☐

Protected Management Frame

PMF Association Comeback Timer* SA Query Time*

Fast Transition

Status Over the DS ☐Reassociation Timeout *

Auth Key Mgmt

OWE cannot be enabled with
802.1X/FT+802.1X/802.1X-SHA256/PSK/FT+PSK/PSK-
SHA256/CCKM/SAE/FT+SAE

SAE ☐FT + SAE ☐OWE ☒FT + 802.1X ☐802.1X-SHA256 ☒Transition Mode WLAN ID

Cancel

Update & Apply to Device

图10:在OWE SSID中启用其他身份验证方法时收到错误消息

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

☐ WPA + WPA2

☐ WPA2 + WPA3

☒ WPA3

☐ Static WEP

☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

WPA2 Policy

☐

GTK Randomize

☐

WPA3 Policy

☒

Transition Disable

☐

Fast Transition

Status

Enabled ▼

Over the DS

☐

Reassociation Timeout *

20

WPA2/WPA3 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Required ▼

Association Comeback Timer*

1

SA Query Time*

200

Auth Key Mgmt

Fast Transition needs to be disabled

OWE cannot be enabled with
802.1X/FT+802.1X/802.1X-SHA256/PSK/FT+PSK/PSK-SHA256/CCKM/SAE/FT+SAE

SAE

☐

FT + SAE

☐

OWE

☒

FT + 802.1X

☒

802.1X-SHA256

☒

Transition Mode WLAN ID

9

↶ Cancel



Update & Apply to Device

图11:启用AKM时出现错误消息

- 在Cisco IOS® XE 17.9.6 IOS版本中，当选择“WPA2+WPA3”时，您可以在AKM下看到“OWE”选项，但是您会收到错误消息，您不能将OWE与此组合一起使用。

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

☐ WPA + WPA2 ☒ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☐ None

MAC Filtering ☐

Lobby Admin Access ☐

WPA Parameters

WPA Policy ☐ WPA2 Policy ☒
 GTK Randomize ☐ WPA3 Policy ☒
 Transition Disable ☐

Fast Transition

Status
 Over the DS ☐
 Reassociation Timeout *

WPA2/WPA3 Encryption

AES(CCMP128) ☒ CCMP256 ☐
 GCMP128 ☐ GCMP256 ☐

Auth Key Mgmt

WPA2 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X/802.1X AKM and AES cipher, 3. PSK-SHA256/FT-PSK/PSK AKM and AES cipher, 4. CCKM AKM and AES Cipher

OWE is supported with WPA3 (WPA/WPA2 must be disabled)

802.1x ☐ PSK ☐
 CCKM ⚠ ☐ SAE ☐
 FT + SAE ☐ OWE ☒
 FT + 802.1x ☐ FT + PSK ☐
 802.1x-SHA256 ☐ PSK-SHA256 ☐
 Transition Mode WLAN ID

Protected Management Frame

PMF
 Association Comeback Timer*
 SA Query Time*

MPSK Configuration

Enable MPSK ☐

Cancel

Update & Apply to Device

图12:选择WPA2+WPA3时出现错误消息

- 在Cisco IOS® XE 17.12.4版本中，当您选择“WPA2+WPA3”时，在AKM中无法获得“OWE”选

项，

Edit WLAN

⌵

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☐ WPA + WPA2

☒ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy☐

GTK Randomize☐

WPA2 Policy☒

WPA3 Policy☒

Transition Disable☐

WPA2/WPA3 Encryption

AES(CCMP128)☒

GCMP128☐

CCMP256☐

GCMP256☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

WPA2 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X/802.1X AKM and AES cipher, 3. PSK-SHA256/FT-PSK/PSK AKM and AES cipher, 4. CCKM AKM and AES Cipher

WPA3 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X AKM and AES cipher, 3. SAE/FT-SAE/OWE AKM and AES cipher.

802.1X☐

PSK☐

CCKM ⚠☐

SAE☐

FT + SAE☐

FT + 802.1X☐

FT + PSK☐

802.1X-SHA256☐

PSK-SHA256☐

MPSK Configuration

Enable MPSK

☐

↶ Cancel

📄 Update & Apply to Device

图13:错误消息 — 未获得AKM中的OWE选项

故障排除

1. 检查WLAN、OPEN SSID和OWE过渡SSID中的配置必须映射过渡WLAN ID。
2. 广播选项必须在OWE转换SSID中禁用，它只能在OPEN SSID中启用。
3. 检查本文中描述的支持的身份验证/加密/FT方法。
4. 如果WLC端的配置正常，请收集所需的日志和输出以缩小问题范围。

RA跟踪和EPC (嵌入式数据包捕获)

登录到WLC GUI -> Troubleshooting -> Radiative Trace -> Add client wifi MAC address -> Click that clients复选框 —> Start

登录到WLC GUI -> Troubleshooting -> Packet Capture -> Add new file name -> Choose the uplink interface and WMI VLAN/Interface -> Start。

从客户端计算机：如果可能，您可以通过选择WiFi接口安装Wireshark应用并收集数据包捕获。

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.html#anc12>

AIR PCAP

您可以通过使用MAC笔记本电脑或将AP之一配置为嗅探器模式来收集它，请参阅以下链接：

从MAC笔记本电脑：

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-mobility/217042-collect-packet-captures-over-the-air-on.html>

从嗅探器AP:

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217057-configure-access-point-in-sniffer-mode-o.html>

将一台笔记本电脑 (wireshark服务器) 连接到交换机端口，其中必须安装wireshark应用程序，此wireshark服务器必须能够访问WLC WMI接口。如果协议“5555、5000或5556”出现在您的WLC和wireshark服务器之间，则需要在防火墙中允许该协议。

检查安装了wireshark的PC中是否安装了任何“gscaler”，如果不是，请“关闭”并尝试，如果是windows defender之类的防火墙或其中存在的任何内容，请禁用它们，然后尝试收集PCAP。

漫游

当客户端从一个AP漫游到另一个AP时，它需要执行以下步骤：

- 需要发送重新关联/关联 — 取决于客户端请求。
- 需要在关联请求中发送DH(Diffie-Helman)详细信息。

- 客户端可以从AP获取关联响应中的DH详细信息，基于此PMK在客户端和AP中生成。
- AP和客户端之间可以进行4次握手。
- 在OWE中，您无法启用FT，因此不可能使用802.11r。
- 每次客户端漫游时，需要在DH交换后进行关联四次握手。
- 客户端和AP使用自己的PMKID，对于每个AP和客户端来说都是唯一的。
- 如果客户端连接到同一个AP，则它可以使用同一个PMKID。在某些情况下，如果客户端被删除，比AP还多，则可以生成新的PMKID，但是客户端使用相同的PMKID进行4次握手。

示例：

如果客户端连接到同一个AP，则您可以在关联请求和关联响应中看到相同的PMKID。在关联响应中，如果DH使用同一PMKID，则无法查看DH详细信息。

```

8522 2025-01-21 09:51:57.329457 ee:13:e8:a8:cd:5b Cisco_dd:2e:8f 802.11 337 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tr
44117 2025-01-21 09:53:12.847592 ee:13:e8:a8:cd:5b Cisco_dd:2e:8f 802.11 337 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tr
> Frame 8522: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  > Tagged parameters (269 bytes)
    > Tag: SSID parameter set: "OWE-Transition"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: -20, Max: 14
    > Tag: Supported Channels
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 42
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      > Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      > Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
      > RSN Capabilities: 0x00c0
      PMKID Count: 1
    > PMKID List
      PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af
      > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: Supported Operating Classes
    > Tag: Extended Capabilities (11 octets)
    > Tag: VHT Capabilities
    > Tag: Vendor Specific: Samsung Electronics Co.,Ltd
    > Tag: Vendor Specific: Samsung Electronics Co.,Ltd
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
  > Ext Tag: OWE Diffie-Hellman Parameter
    Ext Tag length: 34 (Tag len: 35)
    Ext Tag Number: OWE Diffie-Hellman Parameter (32)
    Group: 256-bit random ECP group (19)
    Public Key: 7c 27 82 bb 4c 77 a9 8c 70 76 d1 fa 2e 34 93 34 7e c1 6d 4c 64 34 5d cc f8 b9 bb 68 b2 12 ff 31

```

图14:使用同一PMKID

```

No. Time Source Destination Protocol Length Sequence Number (BE) PMKID Info
8527 2025-01-21 09:51:57.333153 Cisco_dd:2e:8f ee:13:e8:a8:cd:5b 802.11 245 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af Association Response, SN=784, FN=0, Flags=.....C
> Frame 8527: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
  > Tagged parameters (175 bytes)
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 42
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      > Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      > Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
      > RSN Capabilities: 0x00e8
      PMKID Count: 1
    > PMKID List
      PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af
      > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: BSS Max Idle Period

```

图15:与同一PMKID的关联响应

对于测试，从WLC手动删除此客户端，它再次关联到同一AP，此时，客户端发送同一PMKID，但AP在关联响应中发送DH详细信息。

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44117	2025-01-21 09:53:12.847592	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tr
> Frame 44117: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Request, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (4 bytes) > Tagged parameters (269 bytes) > Tag: SSID parameter set: "OWE-Transition" > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: Power Capability Min: -20, Max: 14 > Tag: Supported Channels > Tag: HT Capabilities (802.11n D1.0) > Tag: RSN Information > Tag Number: RSN Information (48) > Tag length: 42 > RSN Version: 1 > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM) > Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) > Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption > RSN Capabilities: 0x0000 > PMKID Count: 1 > PMKID List > PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128) > Tag: RM Enabled Capabilities (5 octets) > Tag: Supported Operating Classes > Tag: Extended Capabilities (11 octets) > Tag: VHT Capabilities > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element > Ext Tag: OWE Diffie-Hellman Parameter > Ext Tag length: 34 (Tag Len: 35) > Ext Tag Number: OWE Diffie-Hellman Parameter (32) > Group: 256-bit random ECP group (19) > Public Key: ba ba f5 2b f0 a5 4c 02 2f 16 f1 0b ad 95 a0 4f cf 95 79 58 3d dc 77 96 bb b3 59 52 42 25 cf 6f								

图16:删除后，客户端发送了包含DH详细信息的同一PMKID

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44121	2025-01-21 09:53:12.851872	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	266			Association Response, SN=1229, FN=0, Flags=.....C
> Frame 44121: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Response, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) > Tagged parameters (196 bytes) > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: RSN Information > Tag Number: RSN Information (48) > Tag length: 26 > RSN Version: 1 > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM) > Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) > Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption > RSN Capabilities: 0x0000 > PMKID Count: 0 > PMKID List > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > Tag: HT Capabilities (802.11n D1.0) > Tag: HT Information (802.11n D1.0) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: RM Enabled Capabilities (5 octets) > Tag: BSS Max Idle Period > Ext Tag: OWE Diffie-Hellman Parameter > Ext Tag length: 34 (Tag Len: 35) > Ext Tag Number: OWE Diffie-Hellman Parameter (32) > Group: 256-bit random ECP group (19) > Public Key: e4 44 ea 00 6f f3 69 35 33 93 59 3f 7d b7 2e ab d4 04 26 7e 62 da d9 2a 88 c9 4e f5 e2 69 a1 c5								

图17:AP使用DH值生成其新的PMKID

在本例中：AP和客户端在进行4次握手时使用同一个PMKID，请签入“M1和M2”消息。

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
8540	2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193			Key (Message 1 of 4)
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Key (Message 2 of 4)
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267			Key (Message 3 of 4)
8548	2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171			Key (Message 4 of 4)
> Frame 8540: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) > Radiotap Header v0, Length 34 > 802.11 radio information > IEEE 802.11 QoS Data, Flags:F.C > Logical-Link Control > 802.1X Authentication > Version: 802.1X-2004 (2) > Type: Key (3) > Length: 117 > Key Descriptor Type: EAPOL RSN Key (2) > [Message number: 1] > Key Information: 0x0088 > Key Length: 16 > Replay Counter: 0 > WPA Key Nonce: 17 28 f4 7a c2 42 74 21 f3 7f 1b 43 b6 f6 94 71 ea f8 a1 a7 8f eb 2e 10 83 d1 88 c5 a2 e0 5d ed > Key IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 > WPA Key RSC: 00 00 00 00 00 00 00 00 > WPA Key ID: 00 00 00 00 00 00 00 00 > WPA Key MIC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 > WPA Key Data Length: 22 > WPA Key Data: dd 14 00 0f ac 04 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af > Tag: Vendor Specific: Ieee 802.11: RSN PMKID > Tag Number: Vendor Specific (221) > Tag length: 20 > OUI: 00:0f:ac (Ieee 802.11) > Vendor Specific OUI Type: 4 > Data Type: PMKID KDE (4) > PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af								

图 — 18:使用同一PMKID的AP和客户端

在本例中：客户端使用相同的PMKID，但AP使用在客户端被删除后生成的不同PMKID，请检查“M1和M2”消息。

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44128	2025-01-21 09:53:12.857869	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193			Key (Message 1 of 4)
44133	2025-01-21 09:53:12.861273	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	215		21 b5 5d ba b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Key (Message 2 of 4)
44135	2025-01-21 09:53:12.862728	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267			Key (Message 3 of 4)
44138	2025-01-21 09:53:12.865398	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171			Key (Message 4 of 4)

> Frame 44128: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)

> Radiotap Header v0, Length 34

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags:R.F.C

> Logical-Link Control

> 802.1X Authentication

Version: 802.1X-2004 (2)

Type: Key (3)

Length: 117

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 1]

> Key Information: 0x0088

Key Length: 16

Replay Counter: 0

WPA Key Nonce: 17 28 f4 7a c2 42 74 21 f3 7f 1b 43 b6 f6 94 71 ea f8 a1 a7 8f eb 2e 10 83 d1 88 c5 a2 e0 5d ee

Key IV: 00

WPA Key RSC: 00 00 00 00 00 00 00 00

WPA Key ID: 00 00 00 00 00 00 00 00

WPA Key MIC: 00

WPA Key Data Length: 22

> WPA Key Data: dd 14 00 0f ac 04 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f

> Tag: Vendor Specific: Ieee 802.11: RSN PMKID

Tag Number: Vendor Specific (221)

Tag length: 20

OUI: 00:0f:ac (Ieee 802.11)

Vendor Specific OUI Type: 4

Data Type: PMKID KDE (4)

PMKID: 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f

图19:使用不同PMKID的AP和客户端

从内部RA跟踪：

在本例中：客户端在关联请求和AP中发送的DH参数已处理，而不是生成PMK。

```
2025/01/21 15:18:50.157081690 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157082294 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157523328 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157531792 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532236 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532538 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157841380 {wncd_x_R0-0}{1}: [dot11-frame] [21675]: (debug): MAC: ee13.e8a8.cd5b  OW
```

此后，连接到同一AP的同一客户端，此时AP未生成新的PMKID，

```
2025/01/21 15:21:57.391898613 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391903915 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906073 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906329 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。